

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月27日

出 願 番 号

Application Number:

特願2002-282842

[ ST.10/C ]:

[ JP 2002-282842 ]

出 願 人

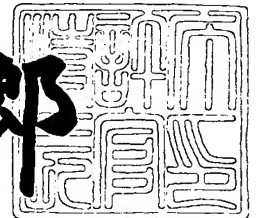
Applicant(s):

新潟大学長

2003年 1月28日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3002086



【書類名】 特許願

【整理番号】 U2002P088

【提出日】 平成14年 9月27日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 7/56

【発明の名称】 乱数発生方法及び乱数発生装置

【請求項の数】 9

【発明者】

    【住所又は居所】 新潟県新潟市五十嵐一の町 7 7 9 4 番地 2 0

    【氏名】 斉藤 義明

【特許出願人】

    【識別番号】 596133441

    【氏名又は名称】 新潟大学長 長谷川 彰

【代理人】

    【識別番号】 100072051

    【弁理士】

    【氏名又は名称】 杉村 興作

【選任した代理人】

    【識別番号】 100059258

    【弁理士】

    【氏名又は名称】 杉村 暁秀

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9812710

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数発生方法及び乱数発生装置

【特許請求の範囲】

【請求項 1】 第 1 のトランジスタと第 2 のトランジスタとを具える双安定性マルチバイブレータ回路に対して駆動電圧を印加することにより、前記第 1 のトランジスタ又は前記第 2 のトランジスタをランダムにオンオフさせ、前記第 1 のトランジスタ又は前記第 2 のトランジスタのオンオフ状態に対応させて 0 又は 1 の数字を割り当て、2 進数的な乱数を発生させるようにしたことを特徴とする、乱数発生方法。

【請求項 2】 前記第 1 のトランジスタ又は前記第 2 のトランジスタの前記オンオフ状態は、前記第 1 のトランジスタ又は前記第 2 のトランジスタのコレクタ電圧を計測することによって検出することを特徴とする、請求項 1 に記載の乱数発生方法。

【請求項 3】 前記双安定性マルチバイブレータ回路の回路部品の特性値を調節することにより、0 及び 1 の生起確率を制御するようにしたことを特徴とする、請求項 1 又は 2 に記載の乱数発生方法。

【請求項 4】 0 及び 1 の生起確率を 0.5 にすることを特徴とする、請求項 3 に記載の乱数発生方法。

【請求項 5】 前記回路部品はバイアス可変抵抗であり、この抵抗の抵抗値を調節することを特徴とする、請求項 3 又は 4 に記載の乱数発生方法。

【請求項 6】 双安定性マルチバイブレータ回路を具えることを特徴とする、乱数発生装置。

【請求項 7】 前記双安定性マルチバイブレータ回路は、バイアス可変抵抗を含むことを特徴とする、請求項 6 に記載の乱数発生装置。

【請求項 8】 前記双安定性マルチバイブレータ回路に接続され、前記双安定性マルチバイブレータ回路に対する駆動電圧を生成するための電源制御回路を具えることを特徴とする、請求項 6 又は 7 に記載の乱数発生装置。

【請求項 9】 前記双安定性マルチバイブレータ回路の前記第 1 のトランジスタ又は前記第 2 のトランジスタのコレクタ側に接続され、前記第 1 のトランジスタ

又は前記第2のトランジスタのコレクタ電圧を取り出すためのバッファ回路を具えることを特徴とする、請求項6～8のいずれか一に記載の乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号作製技術などの情報産業分野、特に将来の量子コンピュータなどの分野において好適に用いることのできる乱数発生方法及び乱数発生装置に関する。

【0002】

【従来の技術】

完全に無秩序であり、かつ全体としては出現頻度が等しくなる乱数は、社会現象や物理現象の数値シミュレーションなどに広く利用されている。また、乱数は暗号技術としても重要な役割を果たしており、情報の保護の分野でもその需要が高い。現在、乱数の発生方法として種々の方法が開発されているが、そのほとんどはアルゴリズムによるソフト的な疑似乱数の生成である。

【0003】

アルゴリズムによる乱数生成は、ある程度の信頼性を有し、高速に乱数生成を行なうことができるという点から広く利用されている。しかしながら、コンピュータは有限の情報しかとらないために、生成された乱数は周期性を持つことが確認されている。そのため、正確な解や十分なセキュリティが得られない場合があり、より無秩序な乱数発生方法の確立が望まれている。

【0004】

近年、ハードウェアの発展に伴う処理速度の向上と信頼性の向上から、物理的な乱数の生成方法が開発されてきた。例えば、熱電子雑音や放射性物質の崩壊などの物理現象に基づいて生成された乱数は、予測不可能性の高い、理想的な乱数列であることが知られている。しかしながら、これらの方法では高価で大掛かりな装置を必要とすることが多い。

【0005】

【発明が解決しようとする課題】

本発明は、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することを目的とする。

【0006】

【課題を解決するための手段】

上記目的を達成すべく、本発明は、第1のトランジスタと第2のトランジスタとを具える双安定性マルチバイブレータ回路に対して駆動電圧を印加することにより、前記第1のトランジスタ又は前記第2のトランジスタをランダムにオンオフさせ、前記第1のトランジスタ又は前記第2のトランジスタのオンオフ状態に対応させて0又は1の数字を割り当て、2進数的な乱数を発生させるようにしたことを特徴とする、乱数発生方法に関する。

【0007】

また、本発明は、双安定性マルチバイブレータ回路を具えることを特徴とする、乱数発生装置に関する。

【0008】

双安定性マルチバイブレータ回路は、一般に個別部品回路の状態であっても集積回路の状態であっても、前記回路を構成する2個のトランジスタの正帰還結合によって構成されている。前記双安定性マルチバイブレータにおいては、駆動電圧を印加した瞬間に、前記2個のトランジスタの一方が導通し、他方は遮断状態となる。したがって、前記2個のトランジスタの特性及び回路部品の特性が完全に一致して、理想的な双安定性マルチバイブレータ回路を構成している場合は、前記2個のトランジスタのどちらが導通するかを予測することは不可能になり、前記双安定性マルチバイブレータ回路内に存在する雑音に依存して決定される。

【0009】

したがって、前記2個のトランジスタの一方の導通状態を検出し、例えば導通状態の場合に数字の“0”を対応させ、遮断状態の場合に数字の“1”を対応させるようにすれば、前記トランジスタのオンオフは前記双安定性マルチバイブレータ回路内に存在する雑音によりランダムとなるから、2進数的な乱数を発生させることができるようになる。

【0010】

なお、前記トランジスタのオンオフ状態は、そのコレクタ電圧を計測することによって簡易に検出することができる。

【0011】

また、上述したような理想的な双安定性マルチバイブレータ回路を構成することができない場合においては、前記トランジスタのオンオフを完全にランダム化することは困難になり、一般には導通状態又は遮断状態のどちらかの状態に偏ることになる。したがって、このような場合においては、上述したような2進数的な乱数を発生させることが困難になる。

【0012】

このような場合においては、前記双安定性マルチバイブレータ回路内の回路部品の特性値を調節し、前記トランジスタのオンオフ状態が前記回路内の雑音に依存してランダムとなるように制御することが好ましい。特に、ある一定期間内でのオンオフ状態が同じ確率でランダムに生じるようにすることが好ましい。これによって、前記期間内での“0”及び“1”の生起確率が0.5となり、2進数的な乱数を発生させることができるようになる。

【0013】

【発明の実施の形態】

以下、本発明を発明の実施の形態に基づいて詳細に説明する。

図1は、本発明の乱数発生装置に含まれる双安定性マルチバイブレータ回路の一例を示す回路図である。図1に示す回路においては、トランジスタT1及びT2、コレクタ抵抗R1及びR2、帰還抵抗R3及びR4、並びにバイアス抵抗R7、R8、R9及びR11が基本的な回路部品であり、コンデンサC1及びC2、抵抗R5及びR6、並びにダイオードD1～D4は波形成形の目的で付加されているものであり、付属的な回路部品である。

【0014】

双安定性マルチバイブレータ回路として機能させるべく、トランジスタT1及びT2は、同一の特性を有するトランジスタから構成する。また、コレクタ抵抗R1及びR2の抵抗値、帰還抵抗R3及びR4の抵抗値、並びにコンデンサC1及びC2のキャパシタは、それぞれ同一となるように設定する。なお、抵抗値R

5 及び R 6、並びにダイオード D 1 ～ D 4 の特性は必ずしも同一とすることは要求されない。但し、一般的にはこれらの回路部品の特性についても同一に設定する。

【 0 0 1 5 】

図 1 に示す双安定性マルチバイブレータ回路に対して所定の駆動電圧を“入力”側から印加すると、トランジスタ T 1 又は T 2 のどちらか一方が導通状態となり、他方が遮断状態となる。このとき、トランジスタ T 1 及び T 2 の特性、コレクタ抵抗 R 1 及び R 2 の抵抗値、帰還抵抗 R 3 及び R 4 の抵抗値、コンデンサ C 1 及び C 2 のキャパシタ、並びにバイアス抵抗 R 8 及び R 9 + R 1 1 の抵抗値が完全に一致していれば、トランジスタ T 1 及び T 2 のオンオフ状態は予測することができず、これらトランジスタのオンオフ状態は双安定性マルチバイブレータ回路内に存在する雑音に依存して決定される。

【 0 0 1 6 】

したがって、トランジスタ T 1 がオンとなって導通状態の時に数字の“0”を対応させ、トランジスタ T 1 がオフとなって遮断状態の時に数字の“1”を対応させるようにする。前述したように、トランジスタ T 1 のオンオフ状態は前記双安定性マルチバイブレータ回路内に存在する雑音に依存するので、“0”及び“1”の数字がランダムに生成され、2進数的な乱数を発生させることができるようになる。

【 0 0 1 7 】

トランジスタ T 1 のオンオフ状態は、例えばトランジスタ T 1 のコレクタ電圧を“出力”側を通じて計測するようにすれば簡易に検出することができる。

【 0 0 1 8 】

しかしながら、上述したような理想的な双安定性マルチバイブレータ回路は、トランジスタ T 1 及び T 2 などの特性を一致するようにした場合においても実現することが困難であり、一般的にはトランジスタ T 1 及び T 2 はオン状態又はオフ状態に傾動する傾向がある。したがって、乱数発生のためのコレクタ電圧を検出すべきトランジスタ T 1 は、導通状態又は遮断状態である場合が遮断状態又は導通状態にある場合よりも多くなり、“0”又は“1”の数字が生起される確率

が“1”又は“0”の数字が生起される確率よりも多くなる。その結果、2進数的な乱数を発生させることができなくなる。

#### 【0019】

このような場合において、双安定性マルチバイブレータ回路内の回路部品の特性を調節することにより、ある一定の期間内において、トランジスタT1及びT2のオンオフ状態が等確率（0.5）で出現するようにする。この場合においては、上述したように、双安定性マルチバイブレータ回路の雑音に依存して、トランジスタT1は、導通状態及び遮断状態をランダムに採るようになるので、これらの状態に“0”及び“1”の数字を割り当てることにより、“0”及び“1”の生起確率は0.5となり、2進数的な乱数を発生できるようになる。

#### 【0020】

図1においては、例えば可変抵抗であるバイアス抵抗R11の抵抗値を制御することによって、トランジスタT1及びT2のオンオフ状態を等確率で出現させることができる。

#### 【0021】

図2は、図1に示す双安定性マルチバイブレータ回路に印加すべき駆動電圧を発生させるための、電源制御回路の一例を示す回路図である。図2に示す電源制御回路は、その出力側を図1に示す双安定性マルチバイブレータ回路の入力側に直列に接続する。

#### 【0022】

図2に示す電源制御回路は、電源より所定のバイアス電流が導入されるとともに、所定の矩形波がコンデンサC3及びC4を介して導入され、トランジスタT3をスイッチング動作させることによって、トランジスタT3のコレクタ側に双安定性マルチバイブレータ回路に対する駆動電圧を発生させ、出力する。なお、コンデンサC3及びC4の代わりに単一の無極性コンデンサを用いることもできる。

#### 【0023】

図3は、図1に示す双安定性マルチバイブレータ回路のトランジスタT1のコレクタ電圧を出力し、計測するために用いるバッファ回路の一例を示す回路図で



ある。図 3 に示すバッファ回路は、その入力を図 1 に示す双安定性マルチバイブレータ回路におけるトランジスタ T 1 のコレクタ側に設けられた出力と接続する。そして、バッファ回路の出力側から計測したコレクタ電圧値を外部に取り出し、所定の演算処理などに供する。

## 【 0 0 2 4 】

このようなバッファ回路を設けることにより、双安定性マルチバイブレータ回路に影響を与えることなく、トランジスタ T 1 のコレクタ電圧値を計測することができるようになる。したがって、2 進数的な乱数を安定的に発生させることができるようになる。

## 【 0 0 2 5 】

図 4 及び図 5 は、図 1 ～図 3 から構成される乱数発生装置を用いて乱数発生の実験を行なった際の実験結果を 2 次元的に表示したものである。図 4 は 5 0 0 0 個の乱数を表し、図 5 は 1 0 0 0 0 個の乱数を表している。図 4 及び図 5 には格子縞などが発生することなく、点状の分布が見られるのみで、2 進数的な乱数が生起されていることが分かる。

## 【 0 0 2 6 】

以上、具体例を挙げながら発明の実施の形態に基づいて本発明を詳細に説明してきたが、本発明は上記内容に限定されるものではなく、本発明の範疇を逸脱しない限りにおいて、あらゆる変形や変更が可能である。

## 【 0 0 2 7 】

例えば、図 1 に示す回路図において、入力端子及びアース間に適当なキャパシタを適当な値に設定したコンデンサ C 1 1 ( 0 . 0 0 1  $\mu$  F )、C 1 2 ( 0 . 1  $\mu$  F ) 及び C 1 3 ( 1  $\mu$  F ) を並列に接続することにより、動作の安定性を向上させることができる。また、上記においてはトランジスタ T 1 のオンオフ状態に対応させて 2 進数的な乱数を発生させたが、トランジスタ T 1 に代えてトランジスタ T 2 を用いることもできる。

## 【 0 0 2 8 】

さらに、トランジスタ T 1 及び T 2 のバランスを取る可変抵抗器 R 1 1 は、抵抗 R 9 に対して直列に接続するのみならず、並列に接続することもできる。また

、 R 1 1 に代えて他の可変抵抗を用い、これを図 1 に示す双安定性マルチバイブレータ回路の任意の抵抗に対して直列又は並列となるように接続するような構成を採ることもできる。

【 0 0 2 9 】

【発明の効果】

以上説明したように、本発明によれば、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することができる。

【図面の簡単な説明】

【図 1】 本発明の乱数発生装置に含まれる双安定性マルチバイブレータ回路の一例を示す回路図である。

【図 2】 双安定性マルチバイブレータ回路に印加すべき駆動電圧を発生させるための、電源制御回路の一例を示す回路図である。

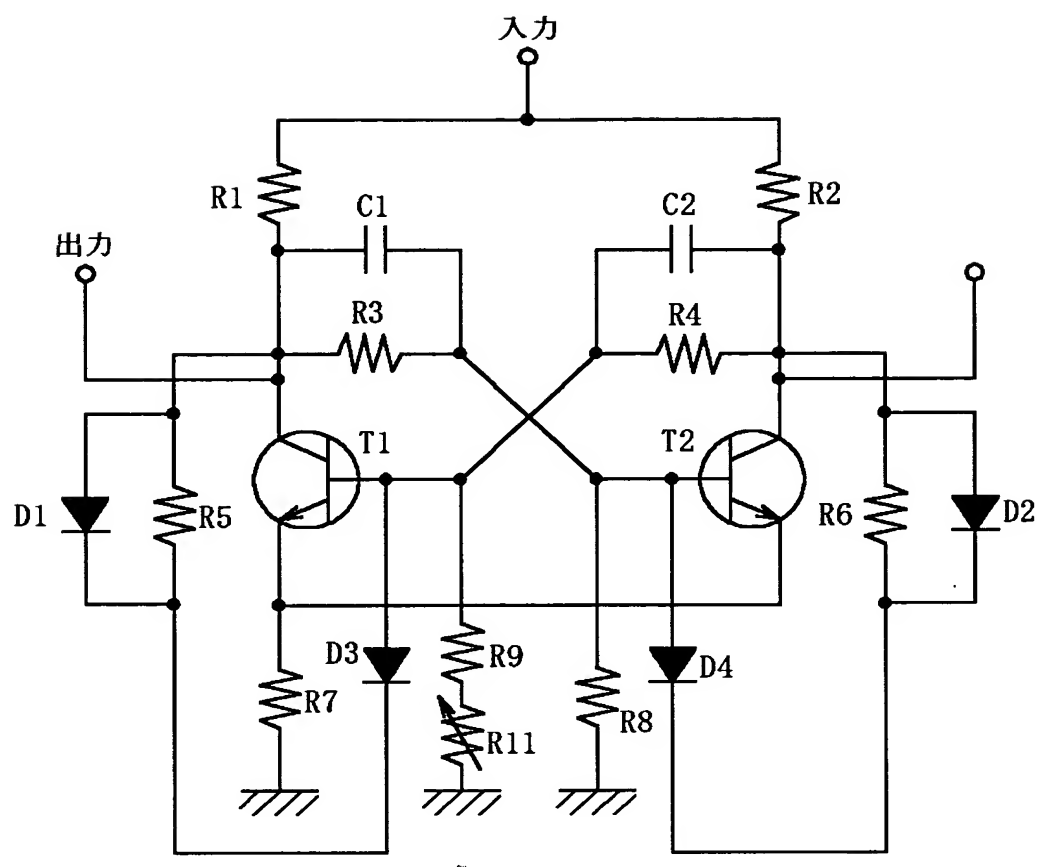
【図 3】 双安定性マルチバイブレータ回路のトランジスタのコレクタ電圧を出力し、計測するために用いるバッファ回路の一例を示す回路図である。

【図 4】 本発明の方法及び装置を用いて生起した乱数の 2 次元度数分布図である。

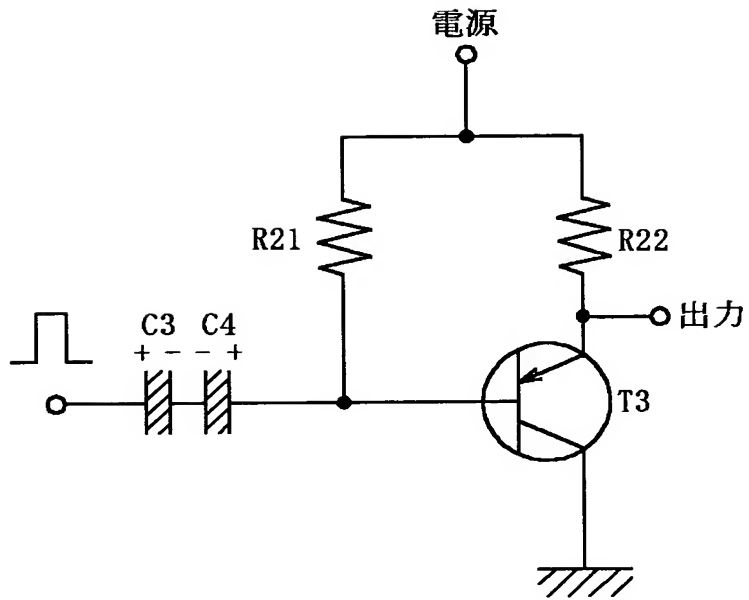
【図 5】 本発明の方法及び装置を用いて生起した乱数の 2 次元度数分布図である。

【書類名】 図面

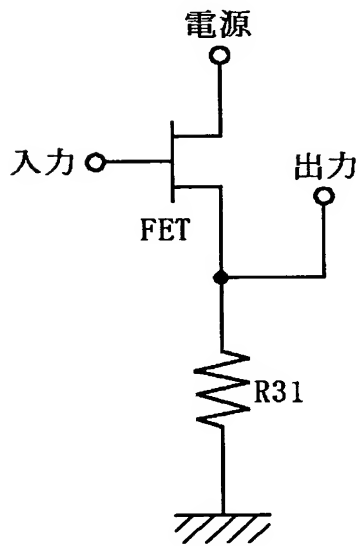
【図 1】



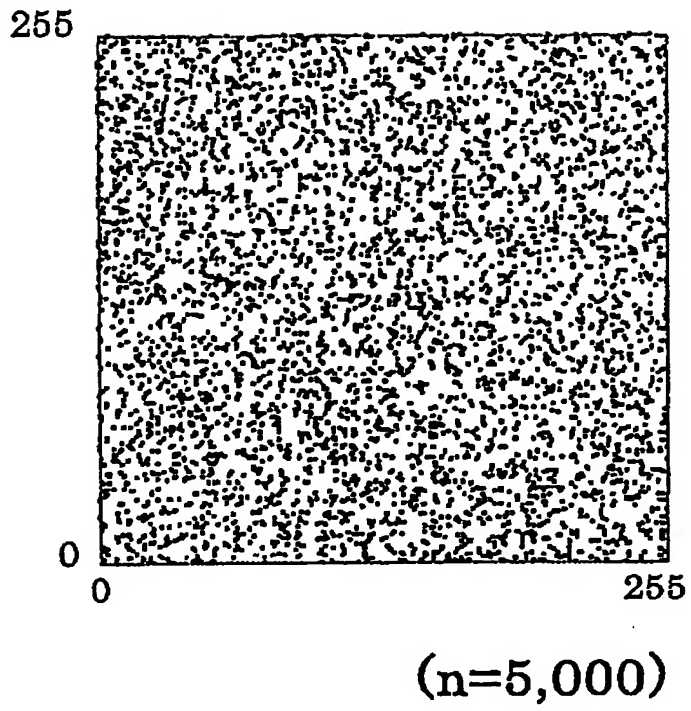
【図 2】



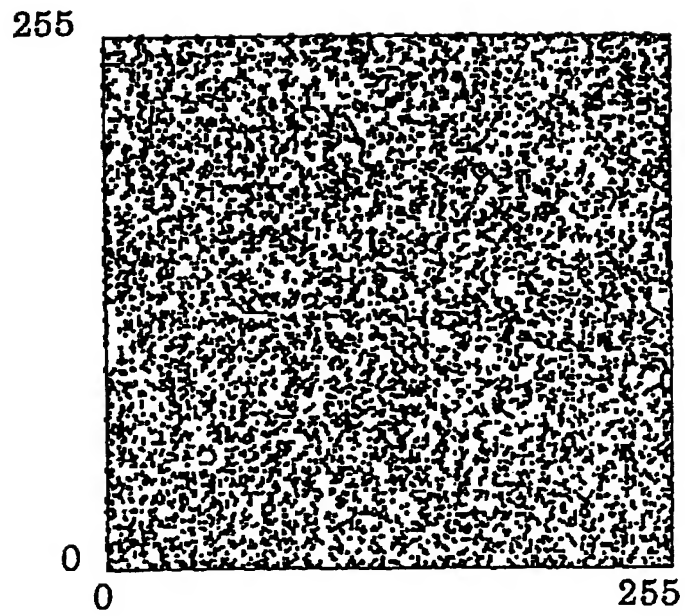
【図 3】



【図 4】



【図 5】



(n=10,000)

【書類名】 要約書

【要約】

【課題】 廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供する。

【解決手段】 双安定性マルチバイブレータ回路に対して所定の駆動電圧を“入力”側から印加して駆動させる。このとき、トランジスタのオンオフ状態は、前記双安定性マルチバイブレータ回路内の雑音に依存してランダムに発生するようになるので、前記トランジスタの導通状態（オン状態）及び遮断状態（オフ状態）に対応させて、数字の“0”及び“1”をそれぞれ対応させることにより、2進数的な乱数を発生させる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2002-282842
受付番号	50201452399
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年 9月30日

<認定情報・付加情報>

【特許出願人】

【識別番号】	596133441
【住所又は居所】	新潟県新潟市五十嵐2の町8050番地
【氏名又は名称】	新潟大学長

【代理人】

申請人	
【識別番号】	100072051
【住所又は居所】	東京都千代田区霞が関3-2-4 霞山ビル7階
【氏名又は名称】	杉村 興作

【選任した代理人】

申請人	
【識別番号】	100059258
【住所又は居所】	東京都千代田区霞が関3-2-4 霞山ビル7階
【氏名又は名称】	杉村 暁秀



出 願 人 履 歴 情 報

識別番号 [ 5 9 6 1 3 3 4 4 1 ]

1. 変更年月日	1 9 9 6 年 9 月 1 1 日
[変更理由]	新規登録
住 所	新潟県新潟市五十嵐 2 の町 8 0 5 0 番地
氏 名	新潟大学長